SFA Due Diligence Checklist

Identification

Where each User of a system that processes or stores SFA data is required to be uniquely identified to the system (usually by the required use of an individually-assigned User ID) to establish accountability.

CRITERIA		EXPECTATIONS	FINDINGS	IN COMPLIANCE?
1	Is each User uniquely identified?	Each User must be identified and authenticated before performing any actions on the system. The use of shared system IDs must be accountable to a specific individual.		
2	Is the User identification limited to 3 attempts?	The authentication process should be limited to three unsuccessful attempts within a 24-hour period. When this limit is reached, the User identifier must be disabled or, if denial of service is a critical issue, authentication attempts may be processed at an increasing time interval. For example, for each failed attempt, the delay before the next log-in prompt increases (e.g., first attempt = 5 seconds, second attempt = 10 seconds, third attempt = 20, fourth attempt = 40, etc.).		
3	Are failed log-in messages non-descriptive?	All messages associated with failed log-ins shall be non-descriptive.		
4*	Are screen blanking mechanisms in place?	A screen blanking mechanism must be activated after a specified period of inactivity. This screen-blanking mechanism must force Users to re-authenticate before any action can take place. The recommended period of inactivity before this mechanism executes is 30 minutes.		
5	Is the User Identification process limited to access from one location only?	A single User identifier must not be permitted to have processes originating from multiple physical locations simultaneously. For example, a user must not have an active session in two different buildings simultaneously.		
6	Is the User identifier disabled if it has been inactive for a period of 60 days.	A User identifier that has been inactive for a period of 60 days must be disabled.		
7*	Is the User identifier purged from the system after 90 days of inactivity and not be reassigned to another user for 6 months.	User identifiers shall be purged from the system after 90 days of inactivity and must not be reassigned to another user for 6 months.		

SFA Due Diligence Checklist

Authenication

Where each User of a system that processes or stores SFA data is required to be authenticated to the system (usually by the required use of password).

	CRITERIA	EXPECTATIONS	FINDINGS	IN COMPLIANCE?
8	Are passwords shared among users?	Authentication information, e.g., password or PIN, must never be disclosed to another User or shared among Users.		
9	Are new or re-enabled User identifiers assigned pre-expired passwords that force the User to change it after the first use?	New or re-enabled User identifiers must be assigned pre-expired passwords that force the User to change it after the first use. These pre-expired passwords must meet all the password controls as an ordinary password would.		
10	Are Passwords documented in any fashion?	Passwords must not be documented in any fashion, such as, written down on printed documents, post-it notes, Email, etc.		
11	Are Passwords protected using an encryption algorithm?	Passwords must be protected using an encryption algorithm. Access to encrypted password files must be restricted.		
12	Do Passwords appear on the screen during the log-in process?	The password must not appear on the screen during the log-in process (The exception to this is during selection of a machine generated password).		
13	Do Passwords have a maximum lifetime of less than 90 days?	Passwords must have a maximum lifetime of 90 days (Exempt from this control are specific system utilities that require password assignment but whose passwords are not used for User authentication, e.g., system monitors).		
14	Does the password change process must force re-authentication?	The password change process must force re-authentication. The current password must be re-entered, followed by the forced creation of a new password. The new password must then be verified by re-entry.		
15*	Is a Password history facility used?	A Password history facility is required to prevent reuse of the previous seven passwords chosen by the User.		
16	Is the minimum length for Passwords seven characters or more?	Passwords are required to be a minimum length of seven characters.		

SFA Due Diligence Checklist

Access to SFA information

Where the system is set up to ensure that Users of a system that processesare only granted access to information or stores SFA data and resources required to support their job function.

CRITERIA		EXPECTATIONS	FINDINGS	IN COMPLIANCE?
17	Is access to information and technology on a need-to-know, job function basis?	Access to information and technology must be on a need-to-know, job function basis. Users must only have the minimum access rights and privileges needed to perform a particular function or transaction.		
18	Are the access rights specified by an individual User?	Access rights specified by an individual User must take precedence over access rights associated with any group the User belongs to (This is also known as Discretionary Access Control).		
19	Is restricted information access controlled?	Access must be controlled to restricted information including:		
		1.Security commands, programs, utilities, and databases		
		2 Program libraries		
		3.Job or process execution statement files		
		4.User authorization profiles		
		5 Accountability tracking logs		
		6.Backup files containing any of the above		
20	Are access control systems documented?	Access control systems must protect SFA data and be documented. These must protect the data from the moment of its being read in until it is destroyed. Documentation must include:		
		1.Who is the "owner" (responsible individual) for the data within the organization		
		2.Who has access to the data		
21	Are user access capabilities changed immediately upon transfer, change of job responsibilities, or leave of absence of a User (employee or third party)?	User access capabilities should be immediately changed upon transfer, change of job responsibilities, or leave of absence of a User (employee or third party).		
22	Are user access capabilities removed immediately upon user's termination of employment?	User access capabilities should be immediately removed upon user's termination of employment.		
23	Is PGP used / available for communications with SFA?	PGP encryption should be in place for communication (including email) with SFA.		

SFA Due Diligence Checklist

Monitoring

The process of gathering information related to compliance with policies and standards and the interaction between users and information.
This information provides a means of reconstructing events for investigative purposes and establishing individual accountability.

CRITERIA		EXPECTATIONS	FINDINGS	IN COMPLIANCE?
24	Do you run system configuration checking tools and intrusion detection tools (e.g., Axent ESM and ITA)	Install and run system configuration checking tools and intrusion detection tools (e.g., Axent ESM and ITA) on systems processing or storing SFA data.		
25	Do you have computer audit logs that record at least unauthorized, and preferably all, accesses to SFA data?	Computer audit logs should record at least unauthorized, and preferably all, accesses to SFA data. These events are:		
		1.Successful and Unsuccessful session log-ins		
		2.Identification and Authentication failures		
		3.Security Administration activity		
		4.All activities performed by privileged Users (users who are able to affect system or data security via their privileges)		
		5.Failed attempts to access information.		
26*	Do you have procedures in place to investigate unauthorized access attempts?	Procedures must be in place to investigate unauthorized access attempts. Specific information must be included in the tracking record associated with each event:		
		1. User identifier		
		2. Information or system accessed		
		3. Date and time of access		
		4. Type and result of event		
		5. Reason for failure (if applicable)		
27	Is the identity of the User, or processes acting on behalf of the User, maintained for the duration of the session?	The identity of the User, or processes acting on behalf of the User, must be maintained for the duration of the session. For example, change of operational mode or privileges should not result in the loss of uniqueness of a user.		
28	Do authentication information, e.g., passwords, PINs, and clear-text cryptographic keys appear as part of the tracking record?	Authentication information, e.g., passwords, PINs, and clear-text cryptographic keys must never appear as part of the tracking record.		
29	Is accountability tracking information maintained for a minimum of one year after it is collected?	Accountability tracking information must be maintained for a minimum of one year after it is collected.		

SFA Due Diligence Checklist

Connectivity

This standard addresses how communications between SFA and the vendor or the communications between a vendor and a third party are established. When systems at SFA or a vendor need to connect to systems at a vendor's location, certain precautions need to be taken.

	CRITERIA	EXPECTATIONS	FINDINGS	IN COMPLIANCE?
30	Is encryption used during connected sessions?	Where SFA data is accessed via the Internet or other untrusted networks, all confidential and sensitive information should be encrypted over the link. PGP (Pretty Good Privacy) can be used for this function, or SFA may agree upon other encryption software		
31	Is access by the vendor’s systems and network to the Internet and SFA systems and network documented.	Any access by the vendors systems and network to the Internet and SFA systems and network must be documented.		
32	Does user authentication used for remote access permit only a finite number of failed access attempts before lockout or disconnection?	User authentication used for remote access must at minimum permit only a finite number of failed access attempts before lock-out or disconnection.		
33	Does authentication use two factor authentication techniques such as SecurID or other tokens supplemented by passwords?	User authentication should preferably use two factor authentication techniques such as SecurID or other tokens supplemented by passwords		
34	Do you check access lists for remote data access to ensure they remain valid?	Access lists for remote data access must be periodically checked to ensure they remain valid (including checking that terminated employees are removed).		
35	Does your facility have a firewall in place?	If computers accessing SFA data are accessible from the Internet, protection by a certified firewall must be in place to protect against unauthorized transfer of data out of the facility. Firewall rules should be available to SFA security at qualification		

SFA Due Diligence Checklist

Media Handling

Vendors are responsible for tracking the release and movement of data. Specifically, when data is received or released the date and location should be logged.

	CRITERIA	EXPECTATIONS	FINDINGS	IN COMPLIANCE?
36	Is media containing SFA data and storage facilities for this data labeled as SFA or SFA customer data?	Media containing SFA data and storage facilities for this data should not be labeled as SFA or SFA customer data.		
37	Is SFA data secured at all times?	SFA data must be properly secured at all times. Under no circumstances should any media be left unattended. Media should be stored in a controlled location where access is limited to people with a business need. Suggested storage areas are as follows:		
		1. File room with physical security.		
		2. Fireproof file cabinet with a combination or lock and key.		
		3. Non-fire proof file cabinet with a combination or lock and key provided backup files are easily accessible and off-site retention period is greater than on-site retention period.		
38	Are media and documents secured at the end of the day or work shift?	All electronic and magnetic media must be removed from work areas and secured at the end of the workday. Additionally, sensitive and confidential paper documents should also be secured at the end of the workday.		
39	Is data that no longer needs to be retained destroyed within 30 days after useful date?	All SFA data that no longer needs to be retained should be destroyed within 30 days after useful date. In addition, paper documentation should also be treated as sensitive information and should also be destroyed if retention is no longer required.		

SFA Due Diligence Checklist

Physical Access

This standard is intended to limit physical access to sensitive equipment and restricted areas throughout SFA to protect systems, both hardware and software, from accidental or intentional damage. This includes, but is not limited to, network systems, servers, tapes, cartridges, microfiche, microfilm, and paper documents. Systems and media, which include customer information, should be deemed as sensitive and treated as such.

	CRITERIA	EXPECTATIONS	FINDINGS	IN COMPLIANCE?
41*	Are all employees issued either a photo ID badge or an access control card-key?	All employees should be issued either a photo ID badge or an access control card-key. Visitors should be issued a badge that identifies them as a non-employee. Employees must display or wear their ID badges or access cards at all times while on the vendor		
42	Are all employees with access to the data center issued either a photo ID badge or an access control card-key?	All data center employees must be issued either a photo ID badge or an access control card-key. Visitors to the data center must be issued a badge that identifies them as a non-employee. Data center employees must display or wear their ID badges or access		
43	Do terminated employees surrender all ID badges and access cards before their departure from the premises.	Terminated employees must surrender all ID badges and access cards before their departure from the premises.		

SFA Due Diligence Checklist

Documentation

This standard addresses the need for adequate documentation and a through understanding of the procedures.

CRITERIA		EXPECTATIONS	FINDINGS	IN COMPLIANCE?
44	Do you have documentation to support your internal operations controls and data security procedures?			
45	Are your documented controls and procedures auditable?			
46	Are your documented procedures updated to reflect the current operating environment?			
47	Are your operational controls independently audited on a periodic basis by either an internal or external auditor?			
48	Do you maintain accurate operational MIS and quality control procedures?			

SFA Due Diligence Checklist

Backup

Vendors are responsible for providing backups for both their hardware and software. Systems and media, which include customer information, should be deemed as senstive and treated as such.

	CRITERIA	EXPECTATIONS	FINDINGS	IN COMPLIANCE?
49	Are procedures to recover the production environment in place?			
50	Are the necessary backup procedures reviewed annually and updated as necessary?			
51	Do you routinely perform backups of system and application software as well as data files?			
52	Does your backup process allow the system to be fully recovered?			
53	Have the data center, operations and business management reviewed and approved the backup procedures, schedules and retention periods at least annually?			
54	Do you have a retention schedule for all backups?			
55	Is your backup facility used for batch processing?			
56	Is your backup recovery tested at least annually?			

SFA Due Diligence Checklist

Contingency Planning

Vendors are responsible for having procedures in place to ensure operations are not comprised by lack of contingency planning. Plans must be in place to ensure smooth operation of business in all situations.

	CRITERIA	EXPECTATIONS	FINDINGS	IN COMPLIANCE?
57	Have you developed data processing and operations contingency plans?			
58	Do you perform a hardware failure analysis at lease semi-annually?			
59	Are your business clients notified during failures to ensure that any critical and immediate business needs are met?			
60	Do you have operating procedures for recovery of full or partial network failures?			

SFA Due Diligence Checklist

Off Site Storage

Any and all SFA information that is stored off site must moved securely be stored in a secure place.

	CRITERIA	EXPECTATIONS	FINDINGS	IN COMPLIANCE?
61	Do you store all data used for processing at your facility?			
62	If you use an off-site storage facility, do they provide at least the same level of security as your company's facility?			
63	Does your tape Llibrarian control the physical movement of information?			
64	If you store information at an off-site facility, do you utilize bonded carrier services to transfer information to and from the offsite location?			
65	Does the offsite facility have a data center?			